NOTICE OF PROPOSED RULEMAKING

Cybersecurity in the Marine Transportation System

May 17, 2024

I. INTRODUCTION

In response to the Department of Homeland Security Coast Guard ("Department") proposed regulation to update its maritime security regulations ("proposed regulation") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike supports the proposed regulation's goal of better protecting U.S. maritime facilities and vessels from cybersecurity threats. These threats continue to evolve and grow more severe. In a recent report, for example, we found that government agencies and related entities remained top targets for cyber attacks in the past year.[1] Furthermore, the report found that nation-state adversaries were active throughout 2023, and continued to operate at an unmatched pace across the global landscape, leveraging stealth and scale to collect targeted group surveillance data, strategic intelligence and intellectual property[2] – making steps to enhance cybersecurity in the sector timely and appropriate.

While we do not have feedback on every aspect of this proposed regulation, we do want to offer several points that may be of value to the Department.

[1] *2024 Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/
[2] Ibid.

A. Cybersecurity Risk Management Practices

We commend the Department for strengthening cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture that would help accomplish the proposed regulation's directive of building a cybersecurity plan that identifies risks, detects threats and vulnerabilities, protects critical systems, and recovers from cyber incidents. The Department notes other guidelines for building cybersecurity baselines such as the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals (CPGs) and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). Harmonization with these documents is important. While these resources offer a security baseline, entities with critical functions, like those within the scope of this proposed rule, often need to take additional, specialized steps to address unique constraints, requirements, and risks.

The proposed regulation already includes some of today's most effective cybersecurity practices. CrowdStrike applauds the inclusion of the following technologies and principles in the proposed regulation and recommends they continue to be included in the final regulation.

- **Identity Protection and Authentication**: As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

As the Department revises the proposed regulation, CrowdStrike recommends the consideration of the following principles and technologies as additional requirements for cybersecurity programs. Notably, several of these practices are also mandated in the May 2021 federal Executive Order (EO) 14028 on Improving the Nation's

Cybersecurity.[3] We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

- **Consideration of Managed Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally. Increasingly, such entities should rely upon managed service providers to achieve the level of security appropriate for listed companies. Organizational transformations along these lines often involve a cross section of departments or teams (*e.g.*, personnel, finance, security, human resources) and can be most expeditiously resolved at the leadership-level.

- **Threat hunting**. Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the *kill chain*. Multiple opportunities for detection help avert "silent failures" -- where a failure of security technology results in security events going completely unnoticed.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.

- **Zero Trust.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. The proposed regulation has MFA requirements to further protect

[3] *Executive Order 14028: Improving the Nation's Cybersecurity*, White House, May 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

entities from identity and credential theft attacks. As the proposed regulation recognizes, due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

- **Next-Generation Security Information and Event Management (SIEM) solutions.** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across a broad array of systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by Endpoint Detection and Response (EDR) tools) and integrate it with other security-relevant event information from an array of sources, powered by AI to deliver to defenders a more cohesive view of what is going on in the environment and an actionable means to defeat threats.

In the *Regulatory Analyses* section of the proposed regulation, the Department states data logging can be achieved with default virus-scanning tools. Due to the importance of logs in detecting and responding to cyber attacks, we recommend the Department accept next-generation logging capabilities, rather than default options that provide limited actionability and accessibility. For example, Falcon LogScale accelerates security operations with petabyte-scale log management and delivers real-time detections and lightning-fast search to stop threats. Choosing an option like Falcon LogScale, likely will save implementers cost over time because it will decrease infrastructure and licensing costs. Next-generation capabilities are highly resistant to tampering, are cryptographically separated from the operating system, and help ensure computer network defenders continue to get the necessary signal from their endpoints.

B. Reporting and Definition Harmonization

The Department seeks public comment on defining a *reportable cyber incident*. It is a welcome distinction that the Department wants to create a higher threshold for an incident that is reportable. The proposed regulation offers a *reportable cyber incident*

definition from the Cyber Incident Reporting Council's model definition in DHS's Report to Congress of September 19, 2023. CrowdStrike supports the Department adopting this definition. The proposed regulation notes the ongoing implementation of Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and its commitment to regulatory harmonization. We applaud the Department's commitment to harmonization and we also recommend alignment where possible with CIRCIA, when rulemaking is finalized and implemented.

The Department also requested input on whether it should require reportable cyber incidents to be reported to CISA. The proposed regulation notes:

> *While this alternative would be a change from current practice, it could allow more efficient use of DHS' cybersecurity resources and may advance the cybersecurity vision laid out by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which will be implemented by regulations that are still under development. Information submitted to CISA would be shared with the Coast Guard, ensuring continued efficient responses.*

Streamlining reporting, where possible, can make reporting an incident easier for a victim while they are trying to respond to an attack.

III. CONCLUSION

The Department's proposed regulation represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. With an emphasis on adoption of practical security practices, these new requirements can raise the already high standard of cybersecurity in the maritime sector. As the Department moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend the Department include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

André Murphy
Senior Federal Technology Strategy Manager

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***